

## UNITED STATES DISTRICT COURT

for the

Southern District of New York

**23 MAG 7090**

In the Matter of the Search of )

(Briefly describe the property to be searched  
or identify the person by name and address) )

All Electronic Devices on the Person of Eric Adams )

Case No. )

**WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Southern District of New York  
(identify the person or describe the property to be searched and give its location):

See Attachment A

The search and seizure are related to violation(s) of (insert statutory citations):

18 USC §§ 371, 666, 1343, and 1349, and 52 U.S.C. § 30121

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment A

**YOU ARE COMMANDED** to execute this warrant on or before November 19, 2023 (not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to \_\_\_\_\_.

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for \_\_\_\_\_ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_.Date and time issued: November 5, 2023 @ 11:19 am


Judge's signature

City and state: New York, New York

Hon. Gary Stein, U.S.M.J.

Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

**Return**

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*

## Attachment A

### I. The Target Subject and the Subject Devices

The Target Subject is New York City Mayor Eric Adams. The Subject Devices include all electronic communications devices found on the person of the Target Subject, including in any garments worn by the Target Subject or in any of his personal effects in his immediate vicinity or control, including bags or containers carried by the Target Subject at the time of the search.

### II. Triggering Condition for the Search of the Target Subject for the Subject Devices

The seizure and search of the Subject Devices authorized by this warrant must be completed at a time not exceeding 14 days from the issuance of this warrant. During that period, the seizure and search of the Subject Devices authorized by this warrant may not be carried out unless the following condition occurs: the Target Subject, Eric Adams, and the Subject Devices, are located in the Southern District of New York.

### III. Seizure and Review of ESI on the Subject Devices

#### A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained on the Subject Devices for evidence, fruits, and instrumentalities of violations of (i) 18 U.S.C. §§ 371 and 666 (theft of federal funds and conspiracy to steal federal funds), (ii) 18 U.S.C. §§ 1343 and 1349 (wire fraud and attempt and conspiracy to commit wire fraud), and (iii) 18 U.S.C. § 371 and 52 U.S.C. § 30121 (campaign contributions by foreign nationals and conspiracy to commit the same) (collectively, the “Subject Offenses”) described as follows:

1. Evidence concerning the identity or location of the owner(s) or user(s) of the Subject Devices.
2. Evidence of knowledge or understanding of, or intent to violate, laws and regulations governing the conduct of the 2021 New York City Mayoral campaign of Eric Adams (the “Adams Campaign”) on the part of [REDACTED] and its employees, officers, or associates (including [REDACTED] the Turkish Government, including its Consulate General in New York and its employees, officers, or associates; or the Adams Campaign.
3. Evidence relating to coordination between [REDACTED] Turkish nationals, or the Turkish Government and the Adams Campaign concerning political contributions to the Adams Campaign, including, but not limited to, evidence of motive and intent for [REDACTED] Turkish nationals, or the Turkish Government to provide or facilitate campaign contributions to the Adams Campaign, and evidence of motive and intent by any person who is or was associated with or employed by the Adams Campaign to provide benefits, whether lawfully or unlawfully, to [REDACTED] Turkish nationals, or the Turkish Government in return for campaign contributions.

4. Evidence relating to payments to employees, officers, and associates of [REDACTED] to facilitate those employees, officers, and associates making campaign contributions to the Adams Campaign.

5. Evidence relating to the source of funds for payment or reimbursement of employees, officers, and associates of [REDACTED] or other persons serving as conduits for campaign contributions to the Adams Campaign originating from Turkish nationals.

6. Evidence of individuals or entities who donated to the Adams Campaign before or after receiving transfers of funds similar to the amount of the donation.

7. Evidence regarding the identity of any persons or entities involved, wittingly or unwittingly, in straw donations to the Adams Campaign.

8. Evidence of the relationship between and among (i) [REDACTED] (ii) the Turkish Government, or (iii) Turkish nationals covertly contributing to the Adams Campaign, and any person who is or was associated with or employed by the Adams Campaign, including all communications with or about, contact information for, and meetings and appointments with co-conspirators.

9. Evidence of an intent to exchange benefits between the Turkish Government or entities and persons acting at its behest, and any person who is or was associated with or employed by the Adams Campaign, including but not limited to straw donations and any actions taken by any person who is or was associated with or employed by the Adams Campaign on behalf of the Turkish Government, [REDACTED] or entities and persons acting at the behest of the Turkish Government.

10. Evidence regarding any requests by the Adams Campaign for matching funds based on donations from [REDACTED] personnel, or any other straw donors, including any discussions of matching funds.

11. Passwords or other information needed to access the user's online accounts, including encrypted data stored in the Subject Devices.

12. Evidence of the geographic location of users, computers, or devices involved in the commission of the Subject Offenses at times relevant to the Subject Offenses.

13. Evidence concerning efforts to destroy evidence of the Subject Offenses or to devise or coordinate false exculpatory explanations for the conduct underlying the Subject Offenses.

## **B. Accessing ESI**

During execution of the search of the Subject Premises authorized herein, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of Eric Adams to any device found at the premises reasonably believed by law enforcement to be used by Adams; or (2) hold any such device in front of Adams's face and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

### **C. Review of ESI**

Following seizure of any electronic communications devices and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the device was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Section III.A of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

UNITED STATES DISTRICT COURT

for the  
Southern District of New York

23 MAG 7090

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

All Electronic Devices on the Person of Eric Adams

Case No.

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Southern District of New York, there is now concealed (identify the person or describe the property to be seized):

Please see Attached Affidavit and its Attachment A

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 371, 666, 1343, 1349; 52 USC 30121	Theft of federal funds, wire fraud, campaign contributions by foreign nationals, and conspiracy to commit these offenses

The application is based on these facts:

See Attached Affidavit and its Attachment A

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ \_\_\_\_\_ (by GS w/ permission)

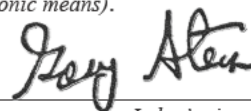
Applicant's signature

Special Agent \_\_\_\_\_ FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
\_\_\_\_\_ telephone (specify reliable electronic means).

Date: 11/05/2023



Judge's signature

City and state: New York, New York

Hon. Gary Stein, U.S.M.J.

Printed name and title



**23 MAG 7090**

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States Of America for a Search and Seizure Warrant for All Electronic Devices on the Person of Eric Adams

**TO BE FILED UNDER SEAL**

**Agent Affidavit in Support of  
Application for Search and Seizure  
Warrant**

SOUTHERN DISTRICT OF NEW YORK) ss.:

██████████ being duly sworn, deposes and says:

**I. Introduction**

**A. Affiant**

1. I have been a Special Agent with the Federal Bureau of Investigation (“FBI”) since 2019. I am currently assigned to a public corruption squad of the New York Field Office, where, among other things, I investigate crimes involving illegal campaign contributions, theft of federal funds, and bribery. Through my training and experience, I also have become familiar with some of the ways in which individuals use smart phones and electronic communications, including social media, email, and electronic messages, in furtherance of their crimes, and have participated in the execution of search warrants involving electronic evidence.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the person of Eric Adams, including any garments worn by Adams and his personal effects in his immediate vicinity or control, including bags or containers carried by Adams, and to seize and search any electronic devices (the “Subject Devices”) found pursuant to that search, for the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of

electronically stored information (“ESI”). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

### **B. The Subject Devices**

3. The Subject Devices are defined as any electronic communications devices found on the person of Eric Adams, including in any garments worn by Adams or in any of his personal effects in his immediate vicinity or control, including bags or containers carried by Adams at the time of the search, that are capable of storing the type of information described in Attachment A.

4. I know from my participation in this investigation and my review of publicly available information, among other sources, that Adams is currently the Mayor of New York City, and as such, he works in an office located in lower Manhattan and is regularly found in the Southern District of New York. Based on my discussions with another law enforcement officer who is involved in providing security for the New York City Marathon being held on November 5, 2023, I know that Adams is expected to be at the finish line of the Marathon, in Manhattan, at approximately 11:30 a.m. or 12:00 p.m. on November 5, 2023. This application seeks authority to execute the search only if Adams is found in the Southern District of New York, and the proposed warrant contains a triggering condition to that effect.

### **C. The Subject Offenses**

5. For the reasons detailed below, I respectfully submit that there is probable cause to believe that the Subject Devices contain evidence, fruits, and instrumentalities of violations of (i) 18 U.S.C. §§ 371 and 666 (theft of federal funds and conspiracy to steal federal funds), (ii) 18 U.S.C. §§ 1343 and 1349 (wire fraud and attempt and conspiracy to commit wire fraud), and (iii)



18 U.S.C. § 371 and 52 U.S.C. § 30121 (campaign contributions by foreign nationals and conspiracy to commit the same) (collectively, the “Subject Offenses”).

## II. Probable Cause

### A. Probable Cause Regarding Subjects’ Commission of the Subject Offenses

6. On November 1, 2023, the Honorable James B. Clark III, United States Magistrate Judge for the District of New Jersey, issued a warrant authorizing a search of the home of [REDACTED] [REDACTED] who as discussed below is a member of Adams’s staff, for evidence of the Subject Offenses, including any electronic devices used by [REDACTED]. The search warrant, and the application for that warrant, including the affidavit in support (the “[REDACTED] Premises Affidavit”) are attached as Exhibit A and incorporated by reference herein.

7. As described in greater detail in the [REDACTED] Premises Affidavit, since in or about August 2021, the FBI and the Office of the United States Attorney for the Southern District of New York have been investigating the possible receipt of so-called “straw” donations by the 2021 New York City mayoral campaign of Eric Adams (the “Adams Campaign”) from employees of [REDACTED] a construction company that operates in New York City.<sup>1</sup> Based on my review of publicly available information, among other sources, I know that [REDACTED] is affiliated with a larger Turkish company and many of its employees are Turkish nationals. As detailed in the [REDACTED] Premises Affidavit, Turkey’s Consul General in New York was involved in arranging a [REDACTED] fundraiser at which straw donations (the “Straw Donations”) were made to the Adams Campaign by ten employees of [REDACTED] or relatives of employees of [REDACTED] (the “Straw Donors”), as well as by Erden Arkan, who owns [REDACTED] and was also heavily involved in arranging

---

<sup>1</sup> A straw, or “conduit,” donation occurs when a donation to a political campaign is made in the name of one donor, but the funds in question in fact belong to a different person.

the fundraiser. The Consul General has communicated about this matter with [REDACTED] who was and remains a member of Adams' staff, and Adams has communicated with [REDACTED] about fundraising in the Turkish community and the potential provision of benefits to the Consul General. Adams and members of his staff have intervened in at least one matter within the purview of the New York City government to obtain favorable action for the Consul General. Adams and others associated with him also appear to have received various benefits from persons affiliated with the Consul General, including travel to Turkey via [REDACTED]

8. On November 2, 2023, the FBI executed the search warrant for [REDACTED] home, as well as search warrants for the homes of four other subjects of the investigation—Erden Arkan (owner of [REDACTED] [REDACTED] (a [REDACTED] employee), [REDACTED] (a former [REDACTED] employee), and [REDACTED] (an Adams Campaign fundraiser who, among other things, helped organize the May 7, 2021 fundraiser). At the same time as the searches, the FBI also simultaneously approached eight of the Straw Donors and sought to interview them. Based on my involvement in that operation and my discussions with other law enforcement officers who were also involved, I know, among other things, that some of the subjects of the investigation denied having participated in any scheme, or having made straw donations. Based on the evidence gathered during the investigation, including the evidence described in this affidavit and its exhibits, however, I believe those denials were false. For instance:<sup>2</sup>

a. Arkan acknowledged that [REDACTED] made payments to certain employees shortly before the May 7, 2021 fundraiser, and that those employees then donated the same or

---

<sup>2</sup> Reports of the interviews conducted on November 2, 2023 have not yet been prepared, and the descriptions of interviews that took place that day in this Affidavit are necessarily incomplete, are described in substance and in part, and are intended only to be high-level summaries based on my discussions with other law enforcement officers.

materially similar amounts to the Adams Campaign on May 7, 2021, but denied that there was a connection between those two facts, dismissing them as coincidental.

b. [REDACTED] denied any involvement in a straw donation scheme. She also, among other things, denied having communicated with the Turkish Consul General via Signal (an encrypted messaging application) and denied that the Turkish Consul General had attended a certain dinner with Adams on April 2, 2021. I know, from my review of communications recovered from [REDACTED] cellphone, that she in fact did communicate with the Turkish Consul General via Signal, and that on April 2, 2021, [REDACTED] wrote to the Consul General via WhatsApp “Mr. [REDACTED] thank you for everything,” “the meal was very nice,” “Mr. President asked me to thank you again.” The Consul General responded, on the same date, “You are welcome,” “it was a nice meal.”<sup>3</sup>

c. Some of the Straw Donors denied making donations to the Adams Campaign at all. As noted in the [REDACTED] Premises Affidavit, however, I know from information provided by the New York City Campaign Finance Board that donations were made in the Straw Donors’ names on May 7, 2021. Other Straw Donors acknowledged donating but denied that they made straw donations, claiming, for instance, that the reimbursement received prior to the donations was a reimbursement for miscellaneous corporate expenses and/or was unrelated to any donations to the Adams Campaign. Additionally, one Straw Donor who refused to speak with law enforcement thereafter—according to press reporting—claimed to a journalist that she was “innocent.”

---

<sup>3</sup> These messages were written in Turkish, and the quotations here are from preliminary translations of those messages prepared by FBI linguists.

9. I also know from my involvement in the November 2, 2023 operation and my conversations with other law enforcement officers who were also involved, that others interviewed on November 2, 2023, on the other hand, admitted to their parts in the scheme to make the Straw Donations. For instance, multiple Straw Donors admitted, in substance and in part, that they received payments from [REDACTED] in anticipation of making the Straw Donations to the Adams Campaign in equal amounts, and that they did this at Arkan's direction. For example, [REDACTED] [REDACTED] who was involved in arranging the May 7, 2021 fundraiser at which the Straw Donations were made, admitted, in substance and in part, that her own donation to the Adams Campaign was a straw donation, that she understood that the plan for the May 7, 2021 fundraiser involved making straw donations, and that she assisted in coordinating the Straw Donations at Arkan's direction.

10. I also know from my involvement in this investigation that one of the other subjects whose home was searched on November 2, 2023 was [REDACTED] a fundraiser who worked for the Adams Campaign and who, according to public reporting, is now involved in fundraising for Adams's campaign reelection as mayor. On November 1, 2023, the Honorable Lois Bloom, United States Magistrate Judge for the Eastern District of New York, issued a warrant authorizing a search of [REDACTED] home for evidence of the Subject Offenses, including any electronic devices used by [REDACTED]. The search warrant, and the application for that warrant, including the affidavit in support (the "[REDACTED] Premises Affidavit") are attached as Exhibit B and incorporated by reference herein.

11. Based on my review of pen register data, I know that on the morning of November 2, 2023, [REDACTED] called Adams multiple times, and that one of the calls briefly connected. Based on my participation in the operation on November 2, 2023 and my conversations with other law enforcement officers involved in that operation, I know that those phone calls from [REDACTED] to Adams took place after FBI agents arrived at her residence and knocked on her door, and then

called her when no one answered the door, but before [REDACTED] opened the door and sat for an interview with the FBI. In other words, it appears that when [REDACTED] learned the FBI was at her home and seeking to speak with her, she called Adams before sitting down for an interview with the agents. Further, based on my discussions with an FBI agent who participated in the November 2, 2023 operation, and who seized [REDACTED] phone pursuant to the search warrant discussed in the prior paragraph, I know that shortly after the conclusion of the search of [REDACTED] home, an agent observed that [REDACTED] cellphone received a phone call via Signal, from a contact saved in [REDACTED] phone as “Eric Adams.”

12. Based on my review of public reporting about the searches on November 2, 2023, I believe that Adams became aware of the searches early in the day around the time of the communications with [REDACTED] described in the prior paragraph. According to news accounts, after learning of the searches, Adams canceled his entire schedule for November 2, 2023—despite having traveled that morning to Washington, D.C. for meetings with officials from the administration of the President of the United States—in order to return to New York City.

13. I have spoken to two FBI agents who, on November 3, 2023, conducted an interview of a witness (“Witness-1”) who works as an executive assistant to Adams. During that interview, Witness-1 told the agents, in substance and in part, that on or about November 2, 2023, Witness-1 fielded a call for Adams from [REDACTED]. During that call, [REDACTED] said to Witness-1, in substance and in part, that the FBI had taken [REDACTED] electronic devices, and that [REDACTED] needed to speak with Adams to tell Adams to delete his texts from “something Government,” but Witness-1 could not remember what the “something” was.



**B. Probable Cause Justifying Search of the Subject Devices**

14. As detailed in the [REDACTED] Premises Affidavit and the [REDACTED] Premises Affidavit, both attached as exhibits, there is probable cause to believe that Adams used electronic communications in furtherance of the Subject Offenses. Among other things:

a. As more fully described in both the [REDACTED] Premises Affidavit and the [REDACTED] Premises Affidavit, Adams exchanged a number of messages with both [REDACTED] and [REDACTED] coordinating the scheduling of meeting with individuals associated with Turkey. (*See* Ex. A ¶ 16.c; Ex. B ¶ 16.a).

b. As more fully described in paragraph 17 of the [REDACTED] Premises Affidavit, [REDACTED] and Adams exchanged messages related to the provision of benefits such as luxury travel to Turkey provided to Adams by at least one person who appeared to be acting at the behest of the Turkish Consul General.

c. As more fully described in paragraph 18 of the [REDACTED] Premises Affidavit, an iCloud account used by Adams that was searched pursuant to a search warrant contains a note that appears to concern fundraising for the Adams Campaign and reflect involvement by the Consul General in a “turkish fundraiser.” The search warrant for Adams’s iCloud account was issued on December 2, 2022 by the Honorable Stewart D. Aaron, United States Magistrate Judge for the Southern District of New York, and is, along with the warrant application, attached as Exhibit C and incorporated by reference herein.

d. As more fully described in paragraph 29 of the [REDACTED] Premises Affidavit, Adams exchanged messages with the then-Commissioner of the Fire Department of New York, in which Adams, responding to a request of the Turkish Consul General as relayed by [REDACTED] asked the Commissioner to intervene to ensure that a building used by Turkey’s General Consulate in New York could open despite the lack of adequate fire safety inspections. (*See also*

Ex. A ¶ 16.j (discussing messages between Adams and [REDACTED] on this subject, including, among others, messages in which Adams stated that he had spoken directly to the Consul General about this issue, and messages in which [REDACTED] confirmed that the issue had been resolved and thanked Adams)).<sup>4</sup>

15. Based on my involvement in this investigation, I know that most of Adams's electronic communications discussed above, and in the [REDACTED] Premises Affidavit and the [REDACTED] Premises Affidavit, were sent to/received from a device associated with call number [REDACTED] 3179. That is also the call number associated with the account searched pursuant to the Adams iCloud warrant (*see* Ex. C). However, based on my involvement in this investigation, I know that Adams uses multiple cellphones, and that he has communicated in furtherance of the Subject Offenses on at least one other cellphone number. For instance, some of the text messages discussed in the [REDACTED] Premises Affidavit regarding [REDACTED] the [REDACTED] employee who arranged travel to Turkey for Adams and others associated with him, evidently at the direction of Turkish officials—were exchanged between [REDACTED] and a different cellphone used by Adams. (*See* Ex. A ¶ 17). That cellphone, with call number [REDACTED] 0448 (“Adams’s Second Cellphone”), was associated in [REDACTED] phone with the contact name “Eric Adams #1.” From reviewing [REDACTED] iCloud and the contents of her cellphone, obtained pursuant to search warrants, I know that [REDACTED] messages with Adams using Adams’s Second Cellphone included the following discussions relevant to the Subject Offenses:

a. On or about February 26, 2019, Adams texted [REDACTED] “[REDACTED] run the Turkish president visit by [REDACTED]” and [REDACTED] responded “I did,” “She said confirm with you first

---

<sup>4</sup> In her interview with law enforcement on November 2, 2023, in substance and in part, [REDACTED] acknowledged that Adams assisted the Turkish Consul General in obtaining FDNY approvals for the Turkish Consulate, but denied that it was in exchange for anything.



if you are ok to host him at BH.” (I know from public reporting, among other sources, that at the time of these messages Adams was the Brooklyn Borough President, and based on my involvement in this investigation, I believe “BH” refers to Brooklyn Borough Hall.)

b. On or about March 3, 2019, Adams texted [REDACTED] “We need to the [sic] trip to Turkey after July 11th” and [REDACTED] responded “Ok.”

c. On or about March 14, 2019, [REDACTED] texted Adams “To be in safe side,” “Please Delete all messages you send me.” Adams replied “Always do.”<sup>5</sup>

d. On or about June 10, 2021, Adams and [REDACTED] exchanged messages about a “breakfast with [REDACTED] at “Alibaba Turkish Restaurant” in Manhattan at 7:00 a.m.. A few hours later, [REDACTED] texted Adams “BP,” “Can Turkish consulate share video from today’s breakfast on their website?” “Is that ok for you?” and Adams responded “I would rather not until after the election. We don’t want any negative news story to come from it.”

16. Based on my training and experience, electronic communications, including emails and text messages, are frequently stored on persons’ electronic communications devices, such as cellphones and tablets. In addition, based on my training and experience and my involvement in this investigation, I know that persons often receive information about airline travel, hotel bookings, and financial records, electronically via email or other electronic message, and that as detailed above, that information may reflect the provision or receipt of pecuniary benefits.

17. Electronic files or remnants of such files can be recovered months or even years after they have been created or saved on an electronic device such as the Subject Devices. Even

---

<sup>5</sup> As discussed in this affidavit and in the [REDACTED] Premises Affidavit, despite [REDACTED] instruction to delete messages, a later search of [REDACTED] cellphones nonetheless recovered numerous messages between her and Adams. In my experience, I have learned that people often fail to fully delete messages on their cellphones, whether due to lack of diligence, lack of technical skill, or the ability of forensic software to recover messages the user has attempted to delete.

when such files have been deleted, they can often be recovered, depending on how the hard drive has subsequently been used, months or years later with forensics tools. Thus, the ability to retrieve from information from the Subject Devices depends less on when the information was first created or saved than on a particular user's device configuration, storage capacity, and computer habits.

18. In addition to the evidence discussed above that Adams has used the Subject Devices to communicate about the Subject Offenses, there is probable cause to believe that cellphones and tablets (including Apple iPads) used by Adams will contain evidence of the Subject Offenses for these additional reasons:

a. Tablets and cellphones can be used store documents, including emails, text messages, previous electronic chats, and financial documents like bank statements and travel expenditure. They can also be used to create documents in word processing programs, like Microsoft Word. Document attachments to communications can be saved intentionally or as a result of a cellphone's or tablet's operating system or web browser to an electronic device, including a computer, tablet, or cellphone. Moreover, and more generally, users of cellphones and tablets who are engaged in the commission of the Subject Offenses often store documents relevant to that activity on their devices, and also maintain notes of meetings and telephone calls on their devices. Such documents can include, but are not limited to, Microsoft Word and PDF documents, drafts, scans, bank statements received from financial institutions, and government filings.

b. Cellphones and tablets can contain photographs and videos of meetings—such as the images of [REDACTED] with Adams and [REDACTED] discussed in paragraph 14 of the [REDACTED] Premises Affidavit—and documents, audio recordings of telephone calls and meetings, and screenshots of text messages.

c. Electronic files, or remnants of those files, downloaded to a cellphone or tablet can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensics tools. When a person “deletes” a file on a cellphone, tablet, or computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space—for long periods of time before they are overwritten. In addition, a device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from a cellphone, tablet, or computer depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and cellphone habits.

d. Additionally, a person can transfer data from an old cellphone, tablet, or computer to a new device, including, for example, mail, contacts, calendars, photos and videos, books and pdfs, call logs, and text messages. For individuals who regularly change or upgrade their devices, including cellphones, it is common to transfer electronic records, such as emails, contacts, calendars, photos and videos, books and pdfs, call logs, and text messages from the old phone to a new phone. Individuals can transfer data in a few ways, including in a cellphone provider or Apple store, through a personal computer containing a backup, or through an iCloud

backup. Accordingly, data found on one electronic device is often found on other devices used by the same person.

19. Based on the foregoing, I respectfully submit there is probable cause to believe that the subjects of the investigation described herein committed the Subject Offenses, that Adams has used at least two different electronic devices to exchange communications relevant to the Subject Offenses, and that the evidence, fruits, and instrumentalities of the Subject Offenses listed in Attachment A, which is incorporated by reference herein, will be found on the Subject Devices.

### **III. Procedures for Searching ESI**

#### **A. Review of ESI**

20. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained on the Subject Devices for information responsive to the warrant.

21. In conducting this review, law enforcement may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- “scanning” storage areas to discover and possibly recover recently deleted data or for deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of search terms related to the subject matter of the

investigation. (Keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.)

22. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement may need to conduct a complete review of all the ESI from the Subject Devices to locate all data responsive to the warrant.

#### **B. Accessing ESI**

23. I know from my training and experience, as well as from information found in publicly available materials, that Apple iPhones and iPads offer their users the ability to unlock the device via biometric features (e.g., fingerprint, facial recognition) in lieu of a numeric or alphanumeric passcode or password. Apple's fingerprint recognition feature is called Touch ID, and its facial recognition feature is called Face ID.

24. If a user enables Touch ID on a given device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) found at the bottom center of the front of the device.

25. If a user enables Face ID on a given device, he or she can unlock the device by raising the iPhone to his or her face.

26. In my training and experience, users of devices that offer Touch ID or Face ID often enable it because it is considered to be a more convenient way to unlock the device than by entering

a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents.

27. In some circumstances, Touch ID or Face ID cannot be used to unlock a device that has either security feature enabled, and a passcode or password must be used instead. These circumstances include: (1) when the device has just been turned on or restarted; (2) when more than 48 hours has passed since the last time the device was unlocked; (3) when the passcode or password has not been entered in the last 6 days, and the device has not been unlocked via Touch ID in the last 8 hours or the device has not been unlocked via Face ID in the last 4 hours; (4) the device has received a remote lock command; or (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made.

28. The passcodes or passwords that would unlock electronic devices subject to seizure pursuant to the requested warrant are unknown to law enforcement. Thus, it will likely be necessary to press Adams's fingers to any Touch ID sensors, or to hold those devices in front of Adams's face to activate the Face ID sensor, in an attempt to unlock those devices for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant devices via Touch ID with the use of the fingerprint of the user, or via Face ID by holding the device in front of the user's face, is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

29. Although I do not know which of a given user's 10 fingerprints are capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock any electronic devices as described above within

the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

30. I also know from my training and experience, and my review of publicly available materials that Apple brand devices have a feature that allows a user to erase the contents of the device remotely. By logging into the Internet, the user or any other individual who possesses the user's account information can take steps to completely wipe the contents of the device, thereby destroying evidence of criminal conduct, along with any other information on the device. The only means to prevent this action is to disable the device's ability to connect to the Internet immediately upon seizure, which requires either access to the device itself to alter the settings, or the use of specialized equipment that is not consistently available to law enforcement agents.

31. Due to the foregoing, I request that the Court authorize law enforcement to press Adams's fingers (including thumbs) to the Touch ID of any seized devices, or to hold those devices in front of Adams's face (and, if necessary, to hold Adams in place while holding the electronic devices in front of his face), for the purpose of attempting to unlock the devices via Touch ID or Face ID in order to search the contents as authorized by this warrant.

### **C. Return of the Subject Devices**

32. If the Government determines that the Subject Devices are no longer necessary to retrieve and preserve the data on the device, and that the Subject Devices are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return the Subject Devices, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.



#### IV. Conclusion and Ancillary Provisions

33. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

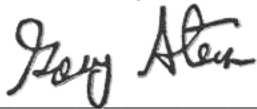
34. In light of the confidential nature of the continuing investigation, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.

/s/ [REDACTED] (by GS w/ permission)

[REDACTED]  
Special Agent  
Federal Bureau of Investigation

Sworn to me through the transmission of this  
Affidavit by reliable electronic means, pursuant to  
Federal Rules of Criminal Procedure 41(d)(3) and 4.1, on

November 5, 2023



HON. GARY STEIN  
UNITED STATES MAGISTRATE JUDGE

## **Attachment A**

### **I. The Target Subject and the Subject Devices**

The Target Subject is New York City Mayor Eric Adams. The Subject Devices include all electronic communications devices found on the person of the Target Subject, including in any garments worn by the Target Subject or in any of his personal effects in his immediate vicinity or control, including bags or containers carried by the Target Subject at the time of the search.

### **II. Triggering Condition for the Search of the Target Subject for the Subject Devices**

The seizure and search of the Subject Devices authorized by this warrant must be completed at a time not exceeding 14 days from the issuance of this warrant. During that period, the seizure and search of the Subject Devices authorized by this warrant may not be carried out unless the following condition occurs: the Target Subject, Eric Adams, and the Subject Devices, are located in the Southern District of New York.

### **III. Seizure and Review of ESI on the Subject Devices**

#### **A. Evidence, Fruits, and Instrumentalities of the Subject Offenses**

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained on the Subject Devices for evidence, fruits, and instrumentalities of violations of (i) 18 U.S.C. §§ 371 and 666 (theft of federal funds and conspiracy to steal federal funds), (ii) 18 U.S.C. §§ 1343 and 1349 (wire fraud and attempt and conspiracy to commit wire fraud), and (iii) 18 U.S.C. § 371 and 52 U.S.C. § 30121 (campaign contributions by foreign nationals and conspiracy to commit the same) (collectively, the “Subject Offenses”) described as follows:

1. Evidence concerning the identity or location of the owner(s) or user(s) of the Subject Devices.

2. Evidence of knowledge or understanding of, or intent to violate, laws and regulations governing the conduct of the 2021 New York City Mayoral campaign of Eric Adams (the “Adams Campaign”) on the part of [REDACTED] and its employees, officers, or associates ([REDACTED] the Turkish Government, including its Consulate General in New York and its employees, officers, or associates; or the Adams Campaign.

3. Evidence relating to coordination between [REDACTED] Turkish nationals, or the Turkish Government and the Adams Campaign concerning political contributions to the Adams Campaign, including, but not limited to, evidence of motive and intent for [REDACTED] Turkish nationals, or the Turkish Government to provide or facilitate campaign contributions to the Adams Campaign, and evidence of motive and intent by any person who is or was associated with or employed by the Adams Campaign to provide benefits, whether lawfully or unlawfully, to [REDACTED] Turkish nationals, or the Turkish Government in return for campaign contributions.

4. Evidence relating to payments to employees, officers, and associates of [REDACTED] to facilitate those employees, officers, and associates making campaign contributions to the Adams Campaign.

5. Evidence relating to the source of funds for payment or reimbursement of employees, officers, and associates of [REDACTED] or other persons serving as conduits for campaign contributions to the Adams Campaign originating from Turkish nationals.

6. Evidence of individuals or entities who donated to the Adams Campaign before or after receiving transfers of funds similar to the amount of the donation.

7. Evidence regarding the identity of any persons or entities involved, wittingly or unwittingly, in straw donations to the Adams Campaign.

8. Evidence of the relationship between and among (i) [REDACTED] (ii) the Turkish Government, or (iii) Turkish nationals covertly contributing to the Adams Campaign, and any person who is or was associated with or employed by the Adams Campaign, including all communications with or about, contact information for, and meetings and appointments with co-conspirators.

9. Evidence of an intent to exchange benefits between the Turkish Government or entities and persons acting at its behest, and any person who is or was associated with or employed by the Adams Campaign, including but not limited to straw donations and any actions taken by any person who is or was associated with or employed by the Adams Campaign on behalf of the Turkish Government, [REDACTED] or entities and persons acting at the behest of the Turkish Government.

10. Evidence regarding any requests by the Adams Campaign for matching funds based on donations from [REDACTED] personnel, or any other straw donors, including any discussions of matching funds.

11. Passwords or other information needed to access the user's online accounts, including encrypted data stored in the Subject Devices.

12. Evidence of the geographic location of users, computers, or devices involved in the commission of the Subject Offenses at times relevant to the Subject Offenses.

13. Evidence concerning efforts to destroy evidence of the Subject Offenses or to devise or coordinate false exculpatory explanations for the conduct underlying the Subject Offenses.

## **B. Accessing ESI**

During execution of the search of the Subject Premises authorized herein, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of Eric Adams to any device found at the premises reasonably believed by law enforcement to be used by Adams; or (2) hold any such device in front of Adams's face and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

### **C. Review of ESI**

Following seizure of any electronic communications devices and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the device was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Section III.A of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

**Exhibit A**  
**[23 MJ 12234]**

**Exhibit B**  
[23 MJ 967]

**Exhibit C**  
**[22 MAG 9730]**



UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All  
Content and Other Information  
Associated with iCloud Account  
[REDACTED] aol.com  
Maintained at Premises Controlled by  
Apple Inc., USAO Reference No.  
2021R00778

**22 MAG 9730**

**SEARCH WARRANT AND NON-DISCLOSURE ORDER**

TO: Apple Inc. ("Provider")

Federal Bureau of Investigation ("Investigative Agency")

**1. Warrant.** Upon an affidavit of Special Agent [REDACTED] of the Federal Bureau of Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the iCloud account [REDACTED] aol.com, maintained at premises controlled by the Provider, contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 30 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

**2. Non-Disclosure Order.** Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or

tampering with evidence, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

**3. Sealing.** It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

12/02/2022  
 \_\_\_\_\_  
 Date Issued

10:47 a.m.  
 \_\_\_\_\_  
 Time Issued



\_\_\_\_\_  
 UNITED STATES MAGISTRATE JUDGE  
 Southern District of New York

## **iCloud Search Attachment A**

### **I. Subject Account and Execution of Warrant**

This warrant is directed to Apple Inc. (the “Provider”), headquartered at 1 Infinite Loop, Cupertino, California 95014, and applies to all content and other information within the Provider’s possession, custody, or control associated with the iCloud account [REDACTED] aol.com (the “Subject Account”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

### **II. Information to be Produced by the Provider**

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Account:

a. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

b. *Device information and settings.* All information about the devices associated with the Subject Account, including but not limited to the Integrated Circuit Card ID (“ICCID”) number, the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), the serial number, customer device settings, and repair history.

c. *Transactional records.* All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations.

d. *Address book information.* All address book, contact list, or similar information associated with the Subject Account.

e. *Call history and voicemails.* All call histories, logs for FaceTime calls, audio voicemails, and visual voicemails associated with the Subject Account.

f. *Text message content.* All text messages (including iMessages, Short Message Service (“SMS”) messages, and Multimedia Messaging Service (“MMS”) messages) sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each text message, and the date and time at which each text message was sent).

g. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email).

h. *Photos and videos.* All photographs or videos associated with the Subject Account, including any photographs or videos found on any iCloud Photo Library, My Photo Stream, or iCloud Photo Sharing service linked to the Subject Account. All associated metadata with any photograph or video including the time and date of creation, the author or creator, the means of its creation, and the GPS location information for where a photo or video was taken.

i. *Documents.* All documents stored in or otherwise associated with the Subject Account, including all documents in iCloud Drive, and iWork Apps.

j. *Search and web histories.* All search history, web history, bookmarks, and iCloud Tabs.

k. *Third-party application data.* All records, messages, and data relating to third-party applications, including WhatsApp and other third-party messaging applications, stored in or otherwise associated with the Subject Account.

l. *Location data.* All location data associated with the Subject Account.

m. *iOS Device Backups.* All device backups, and the contents of those backups, including but not limited to messages, web history, and preferences.

Temporal Limitation. This application is limited to all content created, sent, or received on or after January 1, 2018.

### **III. Review of Information by the Government**

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of theft of federal funds and wire fraud, and conspiracy to commit the same, in violation of 18 U.S.C. §§ 371, 666, 1343, and 1349, including the following:

a. Evidence of knowledge or understanding of, or intent to violate, laws and regulations governing the conduct of the 2021 New York City Mayoral campaign on the part of [REDACTED] and its employees, officers, or associates ([REDACTED] the Turkish Government, including its Consulate General in New York and its employees, officers, or associates; or the 2021 New York City mayoral campaign of Eric Adams and its employees, officers, or associates (the “Adams Campaign”).

b. Evidence relating to coordination between [REDACTED] or the Turkish Government and the Adams Campaign concerning political contributions to the Adams Campaign, including, but not limited to, evidence of motive and intent for [REDACTED] or the Turkish Government to provide or

facilitate campaign contributions to the Adams Campaign, and evidence of motive and intent by Adams, the Adams Campaign, or any employees or associates of Adams or the Adams Campaign to provide benefits, whether lawfully or unlawfully, to [REDACTED] or the Turkish Government in return for campaign contributions.

c. Evidence relating to payments to employees, officers, and associates of [REDACTED] to facilitate those employees, officers, and associates making campaign contributions to the Adams Campaign.

d. Evidence relating to the source of funds for payment or reimbursement of employees, officers, and associates of [REDACTED] for campaign contributions to the Adams Campaign.

e. Evidence of individuals or entities who donated to the Adams Campaign before or after receiving transfers of funds similar to the amount of the donation.

f. Identity of any persons or entities involved, wittingly or unwittingly, in straw donations to the Adams Campaign.

g. Evidence of the relationship between [REDACTED] the Turkish Government, Adams, and/or the Adams Campaign, including all communications with or about, contact information for, and meetings and appointments with co-co-conspirators.

h. Passwords or other information needed to access user's online accounts, including encrypted data stored in the Subject Account

i. Evidence sufficient to establish the owner and user of the Subject Account at times relevant to the Subject Offenses.

j. Evidence of the geographic location of users, computers, or devices involved in the commission of the Subject Offenses at times relevant to the Subject Offenses.